BAB I

PENDAHULUAN

1.1 Latar Belakang

Menurut Khlif, et.al., (2017), semua perusahaan yang terdaftar di Bursa Efek harus mempublikasikan hasil laporan keuangan tahunan mereka. Perusahaan mempunyai tujuan untuk menavigasi lanskap pengungkapan yang terkadang membingungkan dimana terdapat banyak standar (Elshandidy, et al., 2018: 2; Krzus, 2011). Untuk mendukung adanya keterbukaan, pelaporan informasi tersebut harus memiliki nilai yang berkualitas. Laporan keuangan merupakan sumber informasi yang memungkinkan pihak yang mempunyai kepentingan untuk mengetahui kondisi suatu perusahaan (Karina, 2013:39).

Selain laporan keuangan, investor juga menginginkan adanya pelaporan risiko (non keuangan) yang dipublikasikan pada laporan tahunan. Mereka menginginkan pengungkapan organisasi atau perusahaan tersebut mengidentifikasi risiko utamanya dan bagaimana organisasi atau perusahaan berencana untuk mengelola risiko tersebut (Financial Reporting Council, 2017: 3). Manajemen perusahaan juga dapat meningkatkan kepercayaan investor dengan melaporkan risiko terkait yang di alami oleh perusahaan (FRC, 2017).

Risiko sangat penting bagi perusahaan manapun dan merupakan keharusan bagi pebisnis untuk mengidentifikasi, mengevaluasi, mengelola, dan melaporkan

semua jenis risiko yang berguna untuk pengambilan keputusan eksternal yang lebih baik (CIMA, 2008). Risiko merupakan salah satu penyebab utama ketidakpastian dalam suatu organisasi manapun dan dapat bersumber dari berbagai jenis sumber, baik internal maupun eksternal (Epstein, M.J. & Rejc, 2006). Setiap bank mengidentifikasi sejumlah risiko utama yang harus dimitigasi untuk memastikan operasional nya berjalan dengan baik dan sukses. Diseluruh sektor keuangan, semakin banyak bank yang mulai mengidentifikasi risiko dunia maya sebagai risiko prioritas (Harle, et al., 2016: 4).

Seiring dengan berkembangnya teknologi dan perbankan digital dalam dekade terakhir, pelaporan risiko dunia maya telah muncul sebagai hal yang utama. Cara dari menghadapi risiko dunia maya harus dengan meningkatkan keamanan siber yang cukup. Keamanan siber telah menarik banyak perhatian dalam periode sepuluh tahun terakhir. Dalam dunia bisnis, setiap perusahaan mulai khawatir dengan meningkatnya kejahatan di dunia maya, mulai dari mengungkapkan informasi pribadi yang sensitif, menyebabkan gangguan bisnis, atau mencuri rahasia bisnis dari suatu perusahaan terutama setelah serangkaian pelanggaran data profil yang tinggi. Di Indonesia terdapat kasus kejahatan siber yaitu berupa *skimming* pada ATM di Provinsi Bali baru-baru ini di tahun 2021. Pada praktik kejahatan pada kasus *skimming* ini pelaku kejahatan mengganti pin ATM nasabah dengan cara menggunakan kamera tersembunyi lalu memasukan *deep skimmer* pada mesin ATM dengan tujuan untuk merekam data nasbabah saat melakukan transaksi yaitu agar mengetahui PIN kartu ATM. Kejadian serangan siber lain di

Indonesia terjadi pada nasabah bank rekening Jenius bank BTPN, kejadian ini merupakan kejadian pembobolan rekening nasabah bank BTPN dengan jumlah dana Rp. 50 juta. Kejahatan berawal dari adanya panggilan telepon dari pelaku siber dengan alasan meminta data diri nasabah untuk pembaruan sistem dan kartu ATM. Tindakan tersebut merupakan kejahatan siber, Adapun kejahatan siber dengan meminta data pribadi dengan modus lainnnya seperti *phissing, smishing,* dan *vhishing*.

Menurut laporan keamanan siber tahunan baru-baru ini, lebih dari 20% perusahaan yang terkena serangan siber mengalami kehilangan pendapatan secara substansi, basis pelanggan, dan peluang bisnis yang tersedia, dan sebagian besar perusahaan yang terkena serangan telah menghabiskan jutaan dollar untuk meningkatkan teknologi pertahanan dan memperluas serta memperkuat prosedur keamanan serangan siber (CISCO 2017). Oleh karena dampak yang dilihat mempunyai sifat yang signifikan pada nilai dan operasi perusahaan, keamanan siber menjadi salah satu prioritas utama bagi para eksekutif di perusahaan. Sekitar 88% dari Pejabat Eksekutif di AS khawatir bahwa ancaman dunia maya atau siber ini dapat menghambat pertumbuhan pada perusahaan yang terkena serangan (LOOP 2016). Demikian pula, Investor menuntut keterbukaan perusahaan dalam hal risiko keamanan siber dan pelanggan data, dan bagaimana perusahaan menangani risiko tersebut (Shumsky 2016).

Untuk menanggapi kejadian dari ancaman dunia maya yang meningkat, Bursa Efek Indonesia (BEI) mengingatkan dengan cara mensosialisasikan pentingnya

menjaga keamanan siber bagi perusahaan-perusahaan yang terdaftar di BEI. Acara sosialisasi yang diadakan oleh BEI Bersama Direktorat *cyber* Mabes Polri bertujuan untuk memberikan informasi terkait menjaga dari serangan *cyber* dan macam-macam serangan *cyber*. Tujuan berikut mengahasilkan agar perusahaan lebih mempertimbangkan peningkatan keamanan dunia maya serta menjaga bisnis perusahaan. Institut Akuntan Publik Indonesia (IAPI) menjelaskan bahwa professional akuntan mempunyai peran yang sangat penting di dunia bisnis dan pemerintah dalam hal mengidentifikasi dan mengatasi tantangan risiko dari kejahatan siber. Pada saat ini perusahaan-perusahaan dan lembaga menghadapi beragam masalah baru yaitu dari kejahatan siber, seperti *malware,* pemboboland atas data pribadi dan penipuan pembayaran (*fraud*). Di Indonesia Badan Siber dan Sandi Negara Republik Indonesia (BSSN) mengeluarkan panduan keamanan siber pada saat masa pandemic Covid-19. Panduan ini berisi tentang hal-hal yang perlu diperhatikan oleh pengambil kebijakan pada perusahaan. Panduan ini sangat direkomendasikan bagi perusahaan sebagai acuan dalam menjamin keamanan dalam penyelenggaraan kebijakan *work from home*. Panduan berisi tentang indentifikasi dan persiapan, keamanan rantai pemasok, penerapan keamanan siber bagi organisasi, dan keamanan siber bagi pekerja dan pengguna. Sementara itu, pedoman terkait keamanan siber masih memiliki kelemahan hukum berhubungan dengan penyalahgunaan data pribadi. Perkembangan dari teknologi secara pesat pada sektor keuangan yang menimbulkan adanya potensi risiko seperti kejahatan siber juga belum didukung oleh regulasi mengenai bagaimana memitigasi kejadian

kejahatan *cyber* di Indonesia anatar lain disebabkan sampai saat ini belum ada dan masih dalam proses.

Grafik 1. 1 Grafik Serangan Siber di Indonesia

Sumber: Pusat Operasi Keamanan Siber Nasional di Indonesia (2020)

Dari grafik diatas menunjukan adannya peningkatan serangan siber yang terjadi di Indonesia pada masa pandemic Covid-19. Peningkatan serangan siber mencapai 300% dari tahun sebelumnya, hal tersebut membuat industri perbankan harus menjaga system operasionalnya agar dapat mencegah terjadinya serangan siber.

Berdasarkan penelitian-penelitian yang dilakukan sebelumnya menunjukkan bahwa *Risk Disclosure* (RD) berpengaruh terhadap kinerja keuangan. Hasil dari penelitian Kimathi et al., (2017) menunjukan bahwa *Risk Disclosure* mempunyai pengaruh yang positif terhadap kinerja perusahaan pada perusahaan yang terdaftar di Bursa Efek Kenya. Hasil studi Nahar et al., (2016)

juga menunjukan adanya pengaruh positif pada pengungkapan risiko pada laporan keuangan terhadap kinerja bank pada perusahaan perbankan di negara Bangladesh. Penelitian lain yang dilakukan oleh Oluwagbemiga, (2014) menghasilkan adanya hubungan positif antara pengungkapan risiko operasional, risiko keuangan dan risiko strategis terhadap kinerja perusahaan yang terdaftar di Bursa Efek Nigeria.

Penelitian ini merupakan replikasi dari penelitian yang dilakukan oleh (Atandi, 2017) yang mengunakan obyek perusahaan yang terdaftar di Bursa Efek Kenya yang menunjukkan berhubungan positif khususnya pengungkapan risiko cyber terhadap kinerja keuangan perusahaan. Berbeda dengan studi sebelumnya, studi kali ini memiliki beberapa kontribusi (research gap) dalam beberapa hal. Pertama, pengukuran pengungkapan risiko dunia maya menggunakan data *analysis content*. Kedua, memfokuskan pada pengungkapan *cyber risk disclosure* yang dilaporkan setiap bank pada laporan tahunannya. Ketiga, menggunakan data cyber risk dan bank yang listed di OJK pada tahun 2018-2020 sehingga dimungkinkan dapat membandingka periode normal (2018-2019 dan new normal (2020).

1.2 Identifikasi Masalah

Berdasarkan fenomena pada latar belakang yang telah dipaparkan diatas, menyebutkan bahwa dalam dekade terakhir ini risiko dunia maya atau kejahatan siber termasuk kedalam risiko yang dianggap utama dalam sebuah perusahaan dan dikatakan cukup membuat prihatin dalam dunia bisnis maupun hal lain. Dan

selama mewabahnya Covid-19 bisa dikatakan hal ini makin membuat prihatin dan sangat dapat mempengaruhi kinerja dalam suatu perusahan dikarenakan aktifitas operasional perusahaan terganggu dan dapat merusak operasional serta keuntungan suatu perusahaan tersebut dalam beroperasi.

1.3 Pembatasan Masalah

Ada beberapa batasan masalah dalam penilitian ini, sebagai berikut:

1. Pengukuran *cyber* menggunakan data *analysis content* yang menyertakan data dengan pengelompokan *cyber* sebagai risiko operasionalnya.
2. Pengukuran Profitabilitas menggunakan ROA dan ROE
3. Sample yang diambil yaitu bank yang terdaftar atau *listed* di IDX.
4. Periode yang digunakan hanya pada tahun 2018-2020.

1.4 Rumusan Masalah

1. Apakah pengungkapan *cyber* berpengaruh terhadap ROA?
2. Apakah pengungkapan *cyber* berpengaruh terhadap ROE?

1.5 Tujuan Penelitian

1. Menganalisis pengaruh pengungkapan *cyber risk* terhadap ROA.
2. Menganalisis pengaruh pengungkapan *cyber risk* terhadap ROE.

1.6 Manfaat Penelitian

Manfaat yang diharapkan dari peneitian ini bermanfaat bagi:

Akademisi

Dengan adanya penelitian ini, diharapkan dapat dijadikan sebagai informasi yang bisa dijadikan suatu referensi untuk penelitian selanjutnya. Memberikan pengetahuan mengenai bank-bank yang terdafar sahamnya di BEI baik konvensional maupun syariah. Penelitian ini sangat bermanfaat untuk mengembangak teori-teori yang telah diterapkan pada masa perkuliahan. Diharapkan dari hasil penilitian ini dapat memberikan manfaat informasi yang sesuai dan dapat mengembangkan skripsi ini agar mendapatkan hasil yang diinginkan bagi perusahaan maupun para investor dalam mengambil keputusan.

Perusahaan/Perbankan

Dalam penelitian ini, dapat membantu para perbankan memberikan gambaran mengenai layanan teknologi dalam mengelompokkan suatu permasalah pada suatau perusahan terutama berkaitan dengan *cyber*, serta membantu dalam mengambil suatu keputusan dalam melakukan pengembangan pada bank berbasis digital.

Investor

Pada penelitian ini, diharapkan dapat berguna untuk para *stakeholder* dalam mengambil suatu keputusan dalam berinvestasi pada perusahaan yang dapat memberikan keuntungan yang baik dan dapat menjadikan jalan keluar dalam mengambil suatu keputusan.

Bagi Regulator

Hasil dari penelitian ini diharapkan dapat memberikan bukti empiris mengenai pentingnya pengungkapan *cyber risk* pada perbankan yang ada di Indonesia. Selain itu, penelitian ini juga diharapkan dapat mendorong pihak regulator yaitu Bank Indonesia dan Otoritas Jasa Keuangan untuk terus memperbaiki peraturan yang sudah ada.

1.7 Sistematika Penulisan

Penyusunan laporan penelitian harus disusun sistematis sehingga tercapainya tujuan laporan penelitian. Dengan demikian penelitian dapat dijelaskan secara sistematis dalam laporan penelitian. Adapun Sistematika Penulisan ini dibagimenjadi 5 bagian:

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan grand theory, kerangka pemikiran, literature review, dan hipotesis.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan subjek dan objek penelitian, sampel, variable dan ukuran variable, model regresi, metode pengumpulan data, metode analisis data.

BAB IV ANALISIS DATA DAN PEMBAHASAN

Bab ini untuk menjelaskan pemaparan hasil dari penelitian yang dilakukan oleh peneliti serta metode-metode yang digunakan untuk melakukan uji persamaan regresi.

BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian yang dilakukan, keterbatasan penelitian dan saran.